REMARKS

Claim Objections

Claim 46 stands objected to for reciting "private key parameters defined by the parameters {seed,}."

Claim 46 has been amended to recite" private key parameters defined by the parameter {seed}." Applicant respectfully submits that Claim 46 is currently in condition for allowance.

Reconsideration and withdrawal of the objection is respectfully requested.

Claim Rejections – 35 U.S.C. §102

Claims 1, 26, 32, 54, 67, and 68 stand rejected under 35 U.S.C. §102(b) as being anticipated by Quisquater et al. ("Fast Decipherment Algorithm for RSA Public-Key Cryptosystem").

Directing Examiner's attention to MPEP 2131, the threshold issue under Section 102 is whether the Examiner has established a *prima facie* case for anticipation. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ 2d 1051, 1053 (Fed. Cir. 1987)". "The identical invention must be shown in as complete detail as is contained in the ...claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1566 (Fed. Cir. 1989).

Claim 1 has been amended to include subject matter from Claim 2, reciting a cryptosystem private key recovery device comprising "... a set of private key parameters ... wherein said set of private key parameters comprises a parameter k_p, said parameter k_p is derived from k_p (p-1) mod e=1, p is a prime factor of a public modulus, and e is a given public exponent."

Quisquater does not teach the use of a parameter k_p derived from k_p (p-1) mod e=1 as recited in Claim 1. Applicant cannot find, nor does Examiner cite, any description of this parameter and equation in Quisquater.

In fact, on Page 6 of the Office Action dated September 21, 2004, Examiner states that Claim 2 was "found to be allowable based on the subject matter if incorporated into the corresponding independent claims."

Applicant respectfully submits that Quisquater fails to teach each and every element of amended Claim 1, and therefore Claim 1 is currently in condition for allowance.

Reconsideration and withdrawal of the rejection is respectfully requested.

Claim 26 has been amended to include subject matter from Claim 2, reciting a cryptosystem private key recovery device comprising "... a set of private key parameters ... wherein said private key recovery device is configured to recover a private key from said set of stored private key parameters utilizing the equation k_p (p-1) mod e=1, wherein k_p is a private key parameter, p is a prime factor of a public modulus, and e is a given public exponent."

Quisquater does not teach the use of the equation k_p (p-1) mod e=1 as recited in Claim 26. Applicant cannot find, nor does Examiner cite, any description of this equation in Quisquater.

In fact, on Page 6 of the Office Action dated September 21, 2004, Examiner states that Claim 2 was "found to be allowable based on the subject matter if incorporated into the corresponding independent claims."

Applicant respectfully submits that Quisquater fails to teach each and every element of amended Claim 26, and therefore Claim 26 is currently in condition for allowance.

Reconsideration and withdrawal of the rejection is respectfully requested.

Since Claim 32 depends from Claim 26, Applicant respectfully submits that it is also patentable as it contains the same limitations as its parent claim. Applicant respectfully submits that Claim 32 is currently in condition for allowance.

Reconsideration and withdrawal of the rejection is respectfully requested.

Claim 54 has been amended to include all of the limitations of Claim 55. On Page 6 of the Office Action dated September 21, 2004, Examiner states that Claim 55 was "found to be allowable based on the subject matter if incorporated into the corresponding independent claims." Therefore, Applicant respectfully submits that Claim 54 is currently in condition for allowance.

Reconsideration and withdrawal of the rejection is respectfully requested.

Claim 67 has been amended to include subject matter from Claim 2. The same arguments made above with respect to the patentability of Claim 1 are applicable to the patentability of Claim 67 as well. Therefore, Applicant respectfully submits that Claim 67 is currently in condition for allowance.

Reconsideration and withdrawal of the rejection is respectfully requested.

Claim 68 has been amended to include subject matter from Claim 55. The same arguments made above with respect to the patentability of Claim 54 are applicable to the patentability of Claim 68 as well. Therefore, Applicant respectfully submits that Claim 68 is currently in condition for allowance.

Reconsideration and withdrawal of the rejection is respectfully requested.

Claim Rejections – 35 U.S.C. §103

Claims 39, 40, 46, and 47 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Quisquater in view of Zhang (US 6,154,541).

Since Claims 39, 40, 46, and 47 depend from Claim 26, Applicant respectfully submits that they are also patentable as they contain the same limitations as their parent claim. Applicant respectfully submits that Claims 39, 40, 46, and 47 are currently in condition for allowance.

Reconsideration and withdrawal of the rejection is respectfully requested.

Newly Presented Claim

Applicant respectfully submits that newly presented Claim 69 finds support in the original disclosure and does not constitute new matter. Furthermore, since Claim 69 depends from Claim 26, Applicant respectfully submits that it is also patentable as it contains the same limitations as its parent claim. Applicant respectfully submits that Claim 69 is currently in condition for allowance.

If the Examiner has any questions regarding this application or this response, the Examiner is requested to telephone the undersigned at 775-586-9500.

Respectfully submitted,
SIERRA PATENT GROUP, LTD.

Dated: February 18, 2005

Kenneth D'Alessandro
Reg. No.: 29,144

Sierra Patent Group, Ltd.
P.O. Box 6149
Stateline, NV 89449
(775) 586-9500
(775) 586-9550 Fax